Amendment to the Claims

1. (previously presented) A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined read access control command for a user;

said system administrator defined read access control command listing a set of Lightweight Directory Access Protocol user attributes selected and controlled by said administrator;

said user selecting a subset from said system administrator defined LDAP user attributes for allowing user defined read access to other users;

providing a user defined access control command attribute read list containing user identifications that are allowed to read said user defined subset of said system administrator defined LDAP user attributes; and

said read access control command referring to said user defined read list at runtime thereby allowing said read user identifications read access to said system administrator defined LDAP user attributes~~.~~;

wherein said read access control command resides in a directory containing said LDAP attributes.

2. (original) The process of Claim 1, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

3. (original) The process of Claim 1, further comprising the steps of:

providing a user defined write list containing user identifications that are allowed to write a specified set of attributes;

providing a system administrator defined write access control command;

said write access control command listing the user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list thereby allowing said write user identifications write access to said user attributes.

4. (original) The process of Claim 3, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed

and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

5. (previously presented) A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing for a user a system administrator defined read access control command that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access, said user selecting a subset of user defined LDAP user attributes from said list for read access to other users;

providing for a user a system administrator defined write access control command that lists LDAP user attributes that said administrator has selected for user defined write access, said user selecting a subset of user defined LDAP user attributes from said list for write access to other users;

providing a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said user defined subset from said LDAP user attributes that said administrator has selected for user defined read access; and

providing a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said user defined subset from said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP user attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

6. (previously presented) A process for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined write access control command for a user;

said system administrator defined write access control command listing a set of Lightweight Directory Access Protocol user attributes selected and controlled by said administrator;

said user selecting a subset from said system administrator defined LDAP user attributes for allowing user defined write access to other users;

providing a user defined access control command attribute write list containing user identifications that are allowed to write said user defined subset of said system administrator defined LDAP user attributes; and

said write access control command referring to said user defined write list at runtime thereby allowing said write user identifications write access to said system administrator defined LDAP user attributes.;

wherein said write access control command resides in a directory containing said LDAP attributes.

7. (original) The process of Claim 6, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

8. (original) The process of Claim 6, further comprising the steps of:

providing a user defined read list containing user identifications that are allowed to read a specified set of attributes; and

providing a system administrator defined read access control command;

wherein said read access control command lists the user attributes that said administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

9. (original) The process of Claim 8, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

10. (previously presented) An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a system administrator defined read access control command for a user;

means for said system administrator defined read access control command listing a set of Lightweight Directory Access Protocol (LDAP) user attributes selected and controlled by said administrator;

means for said user selecting a subset from said system administrator defined LDAP user attributes for allowing user defined read access to other users;

a user defined access control command attribute read list containing user identifications that are allowed to read said user defined subset of system administrator defined LDAP user attributes; and

means for said read access control command referring to said user defined read list at runtime thereby allowing said read user identifications read access to said system administrator defined LDAP user attributes;

wherein said read access control command resides in a directory containing said LDAP user attributes.

11. (original) The apparatus of Claim 10, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

12. (original) The apparatus of Claim 10, further comprising:

a user defined write list containing user identifications that are allowed to write a specified set of attributes; and

a system administrator defined write access control command;

wherein said write access control command lists the user attributes that said administrator has selected for user defined write access; and

wherein said write access control command refers to said user defined write list thereby allowing said write user identifications write access to said user attributes.

13. (original) The apparatus of Claim 12, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

14. (previously presented) An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a system administrator defined read access control command for a user that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access, said user selecting a subset of user defined LDAP user attributes from said list for read access to other users;

a system administrator defined write access control command for a user that lists LDAP user attributes that said administrator has selected for user defined write access, said user selecting a subset of user defined LDAP user attributes from said list for write access to other users;

a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said user defined subset from said LDAP user attributes that said administrator has selected for user defined read access; and

a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said user defined subset from said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

15. (previously presented) An apparatus for a simplified access control language that controls access to directory entries in a computer environment, comprising:

a system administrator defined write access control command for a user;

means for said system administrator defined write access control command listing a set of Lightweight Directory Access Protocol (LDAP) user attributes selected and controlled by said administrator;

means for said user selecting a subset from said system administrator defined LDAP user attributes for allowing user defined write access to other users;

a user defined access control command attribute write list containing user identifications that are allowed to write said user defined subset of system administrator defined LDAP user attributes; and

means for said write access control command referring to said user defined write list at runtime thereby allowing said write user identifications write access to said system administrator defined LDAP user attributes;

wherein said write access control command resides in a directory containing said LDAP user attributes.

16. (original) The apparatus of Claim 15, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

17. (original) The apparatus of Claim 15, further comprising:

a user defined read list containing user identifications that are allowed to read a specified set of attributes;

a system administrator defined read access control command;

wherein said read access control command lists the user attributes that said administrator has selected for user defined read access; and

wherein said read access control command refers to said user defined read list thereby allowing said read user identifications read access to said user attributes.

18. (original) The apparatus of Claim 17, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

19. (previously presented) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined read access control command for a user;

said system administrator defined read access control command listing a set of Lightweight Directory Access Protocol user attributes selected and controlled by said administrator;

said user selecting a subset from said system administrator defined LDAP user attributes for allowing user defined read access to other users;

providing a user defined access control command attribute read list containing user identifications that are allowed to read said user defined subset of said system administrator defined LDAP user attributes; and

said read access control command referring to said user defined read list at runtime thereby allowing said read user identifications read access to said system administrator defined LDAP user attributes.;

wherein said read access control command resides in a directory containing said LDAP attributes.

20.(original) The method of Claim 19, wherein upon a client read access, the directory server selects a specific read access control command according to the attribute being accessed and refers to the read list of the owner of the attribute being accessed to determine if said client has permission to execute said read access.

21.(original) The method of Claim 19, further comprising the steps of:

providing a user defined write list containing user identifications that are allowed to write a specified set of attributes;

providing a system administrator defined write access control command;

said write access control command listing the user attributes that said administrator has selected for user defined write access; and

said write access control command referring to said user defined write list thereby allowing said write user identifications write access to said user attributes.

22.(original) The method of Claim 21, wherein upon a client write access, the directory server selects a specific write access control command according to the attribute being accessed and refers to the write list of the owner of the attribute being accessed to determine if said client has permission to execute said write access.

23.(previously presented) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing for a user a system administrator defined read access control command that lists Lightweight Directory Access Protocol (LDAP) user attributes that said administrator has selected for user defined read access, said user selecting a subset of user defined LDAP user attributes from said list for read access to other users;

providing for a user a system administrator defined write access control command that lists LDAP user attributes that said administrator has selected for user defined write

access, said user selecting a subset of user defined LDAP user attributes from said list for write access to other users;

providing a plurality of user defined access control command attribute read lists containing user identifications that are allowed to read said user defined subset from said LDAP user attributes that said administrator has selected for user defined read access;

providing a plurality of user defined access control command attribute write lists containing user identifications that are allowed to write said user defined subset from said LDAP user attributes that said administrator has selected for user defined write access;

wherein said read access control command and said write access control command reside in a directory containing said LDAP attributes;

wherein when a client read access to one of the LDAP user attributes that said administrator has selected for user defined read access occurs, said read access

control command and the read list of the owner of the attribute being accessed are used to determine if said client has permission to execute said read access; and

wherein when a client write access to one of the LDAP user attributes that said administrator has selected for user defined write access occurs, said write access control command and the write list of the owner of the attribute being accessed are used to determine if said client has permission to execute said write access.

24. (previously presented) A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for a simplified access control language that controls access to directory entries in a computer environment, comprising the steps of:

providing a system administrator defined write access control command for a user;

said system administrator defined write access control command listing a set of Lightweight Directory Access Protocol user attributes selected and controlled by said administrator;

said user selecting a subset from said system administrator defined LDAP user attributes for allowing user defined write access to other users;

providing a user defined access control command attribute write list containing user identifications that are allowed to write said user defined subset of said system administrator defined LDAP user attributes; and

said write access control command referring to said user defined write list at runtime thereby allowing said write user identifications write access to said system administrator defined LDAP user attributes.;

wherein said write access control command resides in a directory containing said LDAP attributes.